POLÍTICA DE SEGURANÇA CIBERNÉTICA DA CAIXA

1. Objetivo

Estabelecer princípios, diretrizes e responsabilidades que norteiam a gestão da Segurança Cibernética, a fim de garantir proteção aos empregados, colaboradores e clientes, ativos de TI, informações e dados custodiados na CAIXA contra ameaças e ataques cibernéticos, salvaguardando seus negócios, patrimônio e garantindo sua sustentabilidade e continuidade.

2. Princípios

Boas práticas

A CAIXA adota as boas práticas do mercado nacional e internacional na definição de seus processos, procedimentos, modelos e sistemas utilizados na segurança cibernética e no gerenciamento de riscos cibernéticos.

Efetividade

As ações e atividades relacionadas ao gerenciamento de riscos e segurança cibernética são realizadas de maneira a alcançar os melhores resultados, com elevado padrão de qualidade, observando a relação custo-benefício e utilidade, de acordo com a natureza, complexidade e dimensão da exposição a riscos cibernéticos da CAIXA.

Transparência na comunicação

CAIXA utiliza-se de informações tempestivas e fidedignas para a tomada de decisões e aprimoramento do risco e segurança cibernética, bem como fornece informações de maneira tempestiva e transparente aos órgãos de controle, fiscalização e sociedade, respeitado o grau de sigilo.

Segurança desde a concepção

Os controles e riscos de segurança cibernética devem ser considerados e influenciar desde a etapa de concepção, prospecção e desenho de produtos e serviços de negócio, bem como soluções, arquiteturas, ferramentas e serviços tecnológicos.

Necessidade de conhecer

Sob o ponto de vista da confidencialidade, os dirigentes, empregados e colaboradores têm acesso apenas aos dados e informações que são necessários ao cumprimento de suas responsabilidades laborais na CAIXA.

Menor privilégio

A concessão de privilégio de acesso aos sistemas de informação e recursos tecnológicos, para um usuário, deve ser o mínimo necessário para realização das tarefas sob sua responsabilidade, com foco em mitigar riscos consequentes de ataques cibernéticos ou ações indevidas de usuários explorando privilégios de acesso não necessários às suas atribuições.

Defesa em profundidade

A proteção pela qual os controles de segurança são dispostos deve obedecer o conceito de camadas de segurança, com foco em aumentar a sua efetividade e, caso um determinado ataque causar uma falha em um dos mecanismos de segurança, outros mecanismos ainda poderão fornecer a segurança necessária para proteção dos sistemas, ativos tecnológicos, dados ou informações da empresa.

Segregação de papéis

Na CAIXA há mais de uma pessoa, equipe ou ambiente envolvidos para realização de uma tarefa, com foco em mitigação de riscos. No contexto da segurança cibernética, possui dois objetivos principais: a) pessoas - prevenção de conflito de interesses (real ou aparente), atos ilícitos, fraude, abuso, erros; b) processo - detecção de falhas de controle que incluem violações de segurança, roubo de informações e burla de controles de segurança.

Falhar com segurança

Em caso de ocorrer falha em recurso de TI, deve ser ativado um tratamento adequado que não coloque em risco a disponibilidade, integridade, confidencialidade e autenticidade das informações.

3. Diretrizes

A CAIXA reconhece que a assunção e o gerenciamento de riscos cibernéticos é parte integrante e fundamental nas atividades de uma instituição inserida em um contexto de crescimento da utilização de recursos tecnológicos e de digitalização do relacionamento com clientes e para isso mantém estruturas de governança e gerenciamento de riscos e segurança cibernética adequadas à natureza e complexidade de suas operações e produtos, e à dimensão de sua exposição a esse tipo de risco.

Buscar constantemente no processo de segurança cibernética a inovação, automação, inteligência e melhores práticas de mercado com foco em mitigar os riscos cibernéticos, reduzir custos operacionais no processo, diminuir os tempos de detecção e resposta, aumentar a disponibilidade dos serviços e dessa forma termos serviços e produtos de negócio mais fortes e com uma boa imagem e reputação perante o público em geral.

O modelo conceitual e funcional a ser seguido na CAIXA é o do framework de segurança cibernética do NIST, cuja fundamentação está baseada no mapeamento de ativos,

vulnerabilidades, ameaças e riscos com objetivo de aperfeiçoar a priorização de ações e investimentos necessários à segurança cibernética.

Instrumentos como o apetite e tolerância a riscos cibernéticos, gerenciamento das informações agregadas aos processos, testes de continuidade de negócios, PTR, compartilhamento de informações sobre incidentes relevantes com o mercado, investimentos em treinamento dos empregados e na cultura de riscos da CAIXA são utilizados para a promoção da resiliência cibernética.

A CAIXA possui estratégias e estruturas para gerenciamento de riscos no tocante aos critérios de decisão quanto à terceirização de serviços, contemplando a governança corporativa e de gestão proporcionais à relevância do serviço a ser contratado e à exposição a riscos.

Compõem as estruturas de gerenciamento de riscos cibernéticos os modelos e sistemas que possibilitam a identificação, mensuração e avaliação dos riscos relevantes incorridos pela CAIXA, inclusive simulações em condições normais e de estresse.

Após o processo de avaliação de riscos, são realizados o tratamento, monitoramento e comunicação de riscos cibernéticos de forma a garantir a retroalimentação das experiências visando o reconhecimento de oportunidades de melhoria do processo de gestão de riscos e do planejamento estratégico da empresa.

Os canais de comunicação com os diversos públicos de interesse, mantêm foco na transparência e conscientização, bem como em atender às legislações em vigor.

As novas estratégias, produtos, serviços, processos, canais e atividades têm seus riscos cibernéticos avaliados previamente, assim como sua adequação ao nível de risco aceito à luz da Declaração de Apetite por Riscos e aos controles da Instituição.

As soluções, arquiteturas e ativos de TI privilegiam a padronização e simplicidade em sua concepção e implantação. A não aplicação dessa diretriz implica em aumento da complexidade e custos nas atividades de suporte e operação face a gama de especificidades técnicas existentes e maior complexidade nas funções de identificação, proteção, detecção, reação e recuperação de ameaças e incidentes cibernéticos.

O treinamento e conscientização em segurança cibernética são objetivos buscados pela empresa de forma contínua e seu escopo de atuação envolve dirigentes, empregados, colaboradores, parceiros e clientes.

Os empregados classificam os dados e informações, com o objetivo de direcionar e dimensionar a proteção.

Garantir a confidencialidade, integridade, disponibilidade, autenticidade e não repúdio de dados e informações é responsabilidade de todos os gestores de produtos e serviços de negócio, bem como das unidades de tecnologia quando prospectando, desenvolvendo,

adquirindo e implantando soluções com o objetivo de garantir esses paradigmas da segurança cibernética e da informação em suas atividades.

Os privilégios de acesso concedidos aos dirigentes, empregados e colaboradores restringem-se apenas àqueles necessários para a execução de suas responsabilidades laborais.

Todo acesso aos sistemas e recursos tecnológicos deve ser controlado, visando a existência de um controle preventivo e reativo eficiente quanto ao acesso a esses recursos da empresa, fazendo-se necessário a implantação de controles de autenticação, autorização e rastreabilidade, de acordo com os padrões vigentes na CAIXA e definidos pela unidade responsável pela Segurança Tecnológica e Cibernética.

Os controles de segurança cibernética implantados para mitigação dos respectivos riscos cibernéticos devem ser graduados de acordo com a criticidade da transação e informação.

A CAIXA combina segurança cibernética, continuidade dos negócios, gestão de crises e resiliência corporativa para responder rapidamente a ameaças, minimizar danos, operar mesmo que sob ataque e garantir um retorno tempestivo à normalidade.

Monitoração contínua de eventos de segurança cibernética em regime 24x7 (24h por dia, 7 dias na semana).

A execução completa de um processo não está atribuída a um único responsável e, para tanto, são observadas questões relativas às atribuições, atividades, ambientes e recursos tecnológicos que lhe são necessários.

Os requisitos e definições para a segregação de atribuições, atividades e ambientes, sob a ótica de segurança cibernética, são claramente definidos na CAIXA por intermédio de normas internas específicas.

Os gestores da primeira linha de defesa são responsáveis por mapear as situações de falha em seus processos e definir o tratamento adequado.